A Dataset to Support Research in the Design of Secure Water Treatment Systems

Conference Paper · October 2016

CITATIONS
14

4 authors, including:

Sridhar Adepu
Singapore University of Technology and Design
33 PUBLICATIONS **204** CITATIONS
SEE PROFILE

Khurum Nazir Junejo
PAF Karachi Institute of Economics & Technology
25 PUBLICATIONS **116** CITATIONS
SEE PROFILE

Aditya Mathur
Purdue University, and Singapore University of Technology and Design
205 PUBLICATIONS **4,351** CITATIONS
SEE PROFILE

A Dataset to Support Research in the Design of Secure Water Treatment Systems

Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo and Aditya Mathur

iTrust, Center for Research in Cyber Security,
Singapore University of Technology and Design,
Singapore

Abstract. This paper presents a dataset to support research in the design of secure Cyber Physical Systems (CPS). The data collection process was implemented on a six-stage Secure Water Treatment (SWaT) testbed. SWaT represents a scaled down version of a real-world industrial water treatment plant producing 5 gallons per minute of water filtered via membrane based ultrafiltration and reverse osmosis units. This plant allowed data collection under two behavioral modes: normal and attacked. SWaT was run non-stop from its "empty" state to fully operational state for a total of 11-days. During this period, the first seven days the system operated normally i.e. without any attacks or faults. During the remaining days certain cyber and physical attacks were launched on SWaT while data collection continued. The dataset reported here contains the physical properties related to the plant and the water treatment process, as well as network traffic in the testbed. The data of both physical properties and network traffic contains attacks that were created and generated by our research team.

Keywords: cyber physical systems, datasets, network traffic, physical properties

1 Introduction

Cyber Physical Systems(CPSs) are built by integrating computational algorithms and physical components for various mission-critical tasks. Examples of such systems include public infrastructures such as smart power grids, water treatment and distribution networks, transportation, robotics and autonomous vehicles. These systems are typically large and geographically dispersed, hence they are being network connected for remote monitoring and control. However, such network connectivities open up the likelihood of cyber attacks. Such possibilities make it necessary to develop techniques to defend CPSs against attacks: cyber or physical. A "cyber attack" refers to an attack that is transmitted through a communications network to affect system behavior with an intention to cause some economic harm. A "physical attack" is on a physical component such as a motor or a pump to disrupt state of the system.

Research efforts in securing CPSs from such attacks have been ongoing. However, there is limited availability of operational data sets in this research community to advance the field of securing CPSs. While there are datasets for Intrusion Detection Systems (IDS), these datasets focus primarily on network traffic. Such datasets include, for example, the DARPA Intrusion Detection Evaluation Dataset [3] and the NSL-KDD99 [2] datasets. These data are a collection of RAW TCP dump collected over a period of time which includes various intrusions simulated in a military network environment. Such datasets are thus not suitable for CPS IDS. The only other publicly available datasets for CPS kown to the authors are provided by the Critical Infrastructure Protector Center at the Mississippi State University (MSU) [4]. Their datasets [4] comprise of data obtained from their Power, Gas and Water testbeds. The power dataset is based on a simulated smart grid whereas their water and gas datasets were obtained from a very small scale laboratory testbed. However, as acknowledged by the authors themselves, these datasets have been found to contain some unintended patterns that can be used to easily identify attacks versus non-attacks using machine learning algorithms. Although the gas dataset was updated in 2015 [4] to provide more randomness, it was obtained from a small scale testbed which may not reflect the true complexity of CPSs. Hence, there is no publicly available realistic dataset of a sufficient complexity from a modern CPS that contains both network traffic data and physical properties of the CPS.

The goal of this paper is to provide a realistic dataset that can be utilised to design and evaluate CPS defence mechanisms. In this paper, we present a dataset obtained from Secure Water Treatment testbed (SWaT).

The main objective of creating this dataset and making it available to the research community is to enable researchers to 1) design and evaluate novel defence mechanisms for CPSs, 2) test mathematical models, and 3) evaluate the performance of formal models of CPS. The key contributions of the paper are as follows:

1. A large scale labelled–normal & attack– dataset collected from a realistic testbed of sufficient complexity.
2. Network traffic and physical properties data.

The remainder of this paper is organised as follows. Section 2 describes the SWaT testbed in which the data collection process was implemented. Section 3 presents the attacks used in this data collection procedure. Section 4 describes the entire data collection process including the types of data collected. The paper concludes in Section 5.

2 Secure Water Treatment (SWaT)

1 gallon = 231 cube inch =3.78 liter
5*3.78=18.9 liter

As illustrated in Figure 1, SwaT is a fully operational scaled down water treatment plant with a small footprint, producing 5 gallons/minute of doubly filtered water. This testbed replicates large modern plants for water treatment such as those found in cities. Its main purpose is to enable experimentally validated

Testbed : a piece of equipment used for testing new machinery, especially aircraft engines.

Fig. 1: Actual Photograph of SWaT testbed

research in the design of secure and safe CPS. SWaT has six main processes corresponding to the physical and control components of the water treatment facility. It has the following six-stage filtration process, as shown in Figure 2.

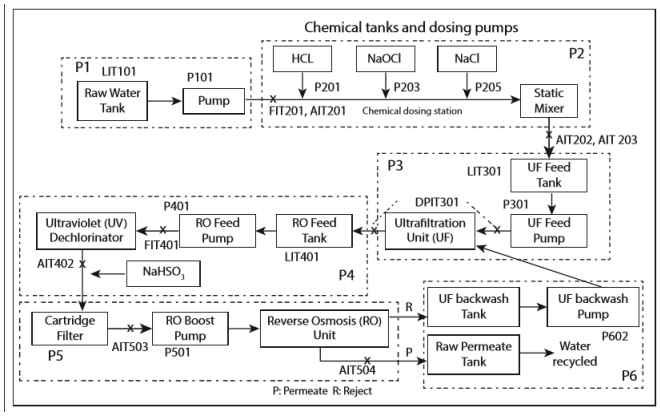


Fig. 2: SWaT testbed processes overview

2.1 Water treatment process

The process (P1) begins by taking in raw water and storing it in a tank. It is then passed through the pre-treatment process (P2). In this process, the qual-

ity of the water is assessed. Chemical dosing is performed if the water quality is not within acceptable limits. The water than reaches P3 where undesirable materials are removed using fine filtration membranes. After the residuals are filtered through the Ultra Filtration system, any remaining chorine is destroyed in the Dechlorination process (P4) using Ultraviolet lamps. Subsequently, the water from P4 is pumped into the Reverse Osmosis (RO) system (P5) to reduce inorganic impurities. In the last process, P6, water from the RO is stored and ready for distribution in a water distribution system. In the case of SWaT, the treated water can be transferred back to the raw tank for re-processing. However, for the purpose of data collection, the water from P6 is disposed to mimic water distribution.

2.2 Communications

SWaT consists of a layered communication network, Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), a Supervisory Control and Data Acquisition (SCADA) workstation, and a Historian. Data from the sensors is available to the SCADA system and recorded by the Historian for subsequent analysis.

As illustrated in Figure 3, there are two networks in SWaT. Level 1 is a star network that allows the SCADA system to communicate with the six PLCs dedicated to each of the process. Level 0 is a ring network that transmits sensor and actuator data to the relevant PLC. The sensors, actuators and PLCs all communicate either via wired or wireless links (where manual switches allow the switch between wireless and wired modes).

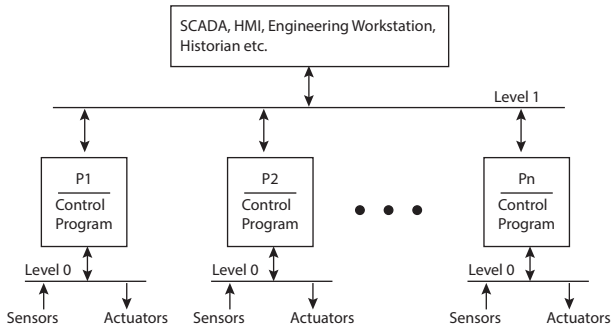


Fig. 3: SWaT testbed processes overview

In the data collection process, only network data through wired communications was collected.

3 Attack Scenarios

A systematic approach was used to attack the system. We used the attack model [1] that considers the intent space of an attacker for a given CPS in the attack model. This attack model can be used to generate attack procedures and functions that target a specific CPS. In our case, the attack model to target the SWaT testbed was derived. We assumed that an attacker succeeds in launching an attack. We assume that an attacker is successful in launching an attack, hence the number of possible attack scenarios is infinite.

The attack model [1] for CPS is abstracted as a sextuple *(M; G; D; P; S_0; S_e)*, where M is potentially an infinite set of procedures to launch attacks, G is a subset of a finite set of attacker intents, D is the domain model for the attacks derived from the CPS, P is a finite set of attack points, and S_0 and S_e are infinite sets of states of CPS, that denote, respectively, the possible start and end states of interest to the attacker. An attack point in CPS could be a physical element or an entry point through the communications network connecting sensors or actuators to the controllers (PLCs) and the SCADA system.

From the above discussion, it is clear that the space of potential attacks is large. The massive size of the attack space arises by changing the method M, potential attack points, P, as well as the start and end state of the CPS. SWaT consists of six stages where each stage contains different number of sensors and actuators. Based on attack points in each stage, the attacks are divided into four types.

1. Single Stage Single Point (SSSP): A Single Stage Single Point attack focuses on exactly one point in a CPS.
2. Single Stage Multi Point (SSMP): A Single Stage Multiple Point attack focuses on two or more attack points in a CPS but on only one stage. In this case set, P consists of more than one element in a CPS selected from any one stage.
3. Multi Stage Single Point (MSSP): A Multi Stage Single Point attack is similar to an SSMP attack except that now the SSMP attack is performed on multiple stages.
4. Multi Stage Multi Point (MSMP): A Multi Stage Multi Point attack is an SSMP attack performed two or more stages of the CPS.

For a detailed description of the attacks generated, we refer the reader to the dataset website[1]. The data collection process consisted of the following steps.
Step 1: Define each attack based on the number of attack points and places.
Step 2: Design each attack based on the attack point (i.e. the actuator or sensor to be affected affect), start state, type of attack, the value of the selected sensor data to be sent to the PLC, the intended impact.

A total of 36 attacks were launched during the data collection process. The breakdown of these attacks are listed in Table 1. The duration of the attack is

[1] `http://itrust.sutd.edu.sg/research/datasets`

varied based on the attack type. A few attacks, each lasting ten minutes, are performed consecutively with a gap of 10 minutes between successive attacks. Some of the attacks are performed by letting the system stabilize before a subsequent attack. The duration of system stabilization varies across attacks. Some of the attacks have a stronger effect on the dynamics of system and causing more time for the system to stabilize. Simpler attacks, such as those that effect flow rates, require less time to stabilize. Also, some attacks do not take effect immediately.

Attack Category	Number of attacks
SSSP	26
SSMP	4
MSSP	2
MSMP	4

Table 1: Number of attacks per category

4 Data collection process

The data collection process lasted for a total of 11 days. SWaT was functioning non-stop 24 hours/day, during the entire 11-day period. SWaT was run without any attacks during the first seven of the 11-days. Attacks were launched during the remaining four days. Various attack scenarios, discussed in Section 3, were implemented on the testbed. These attacks were of various intents and lasted between a few minutes to an hour. Depending on the attack scenario, the system was either allowed to reach its normal operating state before another attack was launched or the attacks were launched consecutively.

The following assumptions ere made during the data collection process.

1. The system will stabilise and reach its operation state within the first seven days of normal operation.
2. Data is recorded once every second assuming that no significant attack on the SWaT testbed can be launched in less than one second.
3. The PLC firmware does not change.

All tanks in SWaT were emptied prior to starting data collection; i.e. the data collection process starts from an empty state of SWaT. This initialization was deemed necessary to ensure that all the tanks are filled with unfiltered water and not pre-treated.

4.1 Physical Properties

All the data was logged continuously once every second into a Historian server. Data recorded in the Historian was obtained from the sensors and actuators of the testbed. Sensors are devices that convert a physical parameter into an electronic output, i.e. an electronic value whereas actuators are devices that convert a signal into a physical output, i.e. turning the pump off or on.

The dataset describes the physical properties of the testbed in operational mode. In total, 946,722 samples comprising of 51 attributes were collected over 11 days. Data capturing the physical properties can be used for profiling cyber-attacks. Table 2 describes the different sensors and actuators in SWaT that served as source of the data.

As the data collection process started from an empty state, it tool about about 5 hours for SWaT to stablise. Figure 4(a) indicates a steady flow of water into the tank in P1 (the level of tank is reported by sensor LIT101). Figure 4(b) shows that it took approximately 5 hours for the tank to fill up and reach its operational state. For the tanks in stages P3 and P4 (level of tank reported by sensor LIT301 and LIT401 respectively), it took approximately 6 hours for the tanks to be filled up. This is because the water from P1 is sent to P2 for chemical dosing before it reaches P3, hence an additional hour is needed to fill up the tank. The water from P3 is subsequently sent to P4 for reverse osmosis.

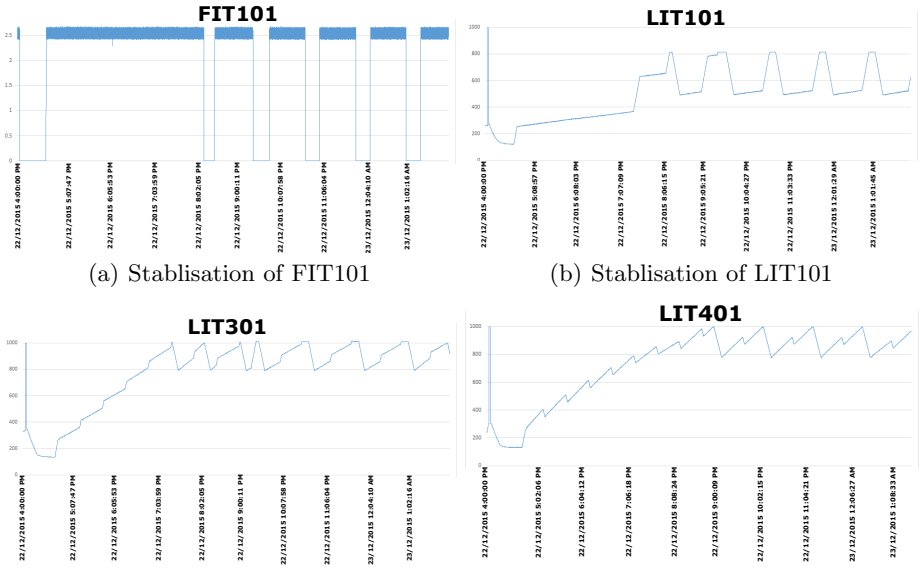
Figures 5(a) and 5(b) illustrate consequences of cyber attacks. Figure 5(a) illustrates a disturbance in the usual cycle of the reading from sensor LIT101 during 6:30 pm and 6:42 pm This was an SSSP attack with the intention of overflowing the tank by shutting pump P101 off and manipulating the value of LIT101 to be at 700mm for 12 minutes. The effects are immediately observed over the next hour before the data stabilised nearly two hours later. Similarly Figure 5(b) shows the consequence of an SSSP attack with the intention to underflow the tank and damage pump P101. In this attack sensor LIT-301 was attacked between 12.08pm and 12.15pm to increase the sensor level to 1100mm. This deceives the PLC to think that there is an over supply of water and turns the pump on to supply water to P4. In reality, the water level falls below the low mark while the pump is still active. Given sufficient time, this attack can cause the tank in P3 to underflow t, thus stagnating the output of the plant and damaging the pumps.

4.2 Network Traffic

Network traffic was collected using commercially available equipment from Check Point® Software Technologies Ltd[2]. This equipment was installed in the SWaT testbed. The use case of the equipment was specifically to collect all the network traffic for analysis. However, for the purpose of data collection, we retrieved

[2] http://us.checkpointsystems.com/

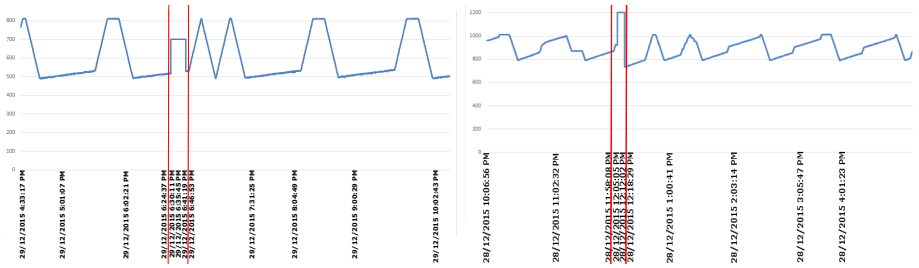
No	Name	Type	Description
1	FIT-101	Sensor	Flow meter; Measures inflow into raw water tank.
2	LIT-101	Sensor	Level Transmitter; Raw water tank level.
3	MV-101	Actuator	Motorized valve; Controls water flow to the raw water tank.
4	P-101	Actuator	Pump; Pumps water from raw water tank to second stage.
5	P-102 (backup)	Actuator	Pump; Pumps water from raw water tank to second stage.
6	AIT-201	Sensor	Conductivity analyser; Measures NaCl level.
7	AIT-202	Sensor	pH analyser; Measures HCl level.
8	AIT-203	Sensor	ORP analyser; Measures NaOCl level.
9	FIT-201	Sensor	Flow Transmitter; Control dosing pumps.
10	MV-201	Actuator	Motorized valve; Controls water flow to the UF feed water tank.
11	P-201	Actuator	Dosing pump; NaCl dosing pump.
12	P-202 (backup)	Actuator	Dosing pump; NaCl dosing pump.
13	P-203	Actuator	Dosing pump; HCl dosing pump.
14	P-204 (backup)	Actuator	Dosing pump; HCl dosing pump.
15	P-205	Actuator	Dosing pump; NaOCl dosing pump.
16	P-206 (backup)	Actuator	Dosing pump; NaOCl dosing pump.
17	DPIT-301	Sensor	Differential pressure indicating transmitter; Controls the back-wash process.
18	FIT-301	Sensor	Flow meter; Measures the flow of water in the UF stage.
19	LIT-301	Sensor	Level Transmitter; UF feed water tank level.
20	MV-301	Actuator	Motorized Valve; Controls UF-Backwash process.
21	MV-302	Actuator	Motorized Valve; Controls water from UF process to De-Chlorination unit.
22	MV-303	Actuator	Motorized Valve; Controls UF-Backwash drain.
23	MV-304	Actuator	Motorized Valve; Controls UF drain.
24	P-301 (backup)	Actuator	UF feed Pump; Pumps water from UF feed water tank to RO feed water tank via UF filtration.
25	P-302	Actuator	UF feed Pump; Pumps water from UF feed water tank to RO feed water tank via UF filtration.
26	AIT-401	Sensor	RO hardness meter of water.
27	AIT-402	Sensor	ORP meter; Controls the $NaHSO_3$dosing(P203), NaOCl dosing (P205).
28	FIT-401	Sensor	Flow Transmitter ; Controls the UV dechlorinator.
29	LIT-401	Actuator	Level Transmitter; RO feed water tank level.
30	P-401 (backup)	Actuator	Pump; Pumps water from RO feed tank to UV dechlorinator.
31	P-402	Actuator	Pump; Pumps water from RO feed tank to UV dechlorinator.
32	P-403	Actuator	Sodium bi-sulphate pump.
33	P-404 (backup)	Actuator	Sodium bi-sulphate pump.
34	UV-401	Actuator	Dechlorinator; Removes chlorine from water.
35	AIT-501	Sensor	RO pH analyser; Measures HCl level.
36	AIT-502	Sensor	RO feed ORP analyser; Measures NaOCl level.
37	AIT-503	Sensor	RO feed conductivity analyser; Measures NaCl level.
38	AIT-504	Sensor	RO permeate conductivity analyser; Measures NaCl level.
39	FIT-501	Sensor	Flow meter; RO membrane inlet flow meter.
40	FIT-502	Sensor	Flow meter; RO Permeate flow meter.
41	FIT-503	Sensor	Flow meter; RO Reject flow meter.
42	FIT-504	Sensor	Flow meter; RO re-circulation flow meter.
43	P-501	Actuator	Pump; Pumps dechlorinated water to RO.
44	P-502 (backup)	Actuator	Pump; Pumps dechlorinated water to RO.
45	PIT-501	Sensor	Pressure meter; RO feed pressure.
46	PIT-502	Sensor	Pressure meter; RO permeate pressure.
47	PIT-503	Sensor	Pressure meter;RO reject pressure.
48	FIT-601	Sensor	Flow meter; UF Backwash flow meter.
49	P-601	Actuator	Pump; Pumps water from RO permeate tank to raw water tank (not used for data collection).
50	P-602	Actuator	Pump; Pumps water from UF back wash tank to UF filter to clean the membrane.
51	P-603	Actuator	Not implemented in SWaT yet.



(a) Stablisation of FIT101 (b) Stablisation of LIT101

(c) Stablisation of LIT301 (d) Stablisation of LIT401

Fig. 4: First 10 hours of data collection



(a) Single point attack on LIT101 (b) Single point attack on LIT301

Fig. 5: Attack Data Plots

network traffic data which is valuable for intrusion detection as in Table 3. Similarly, the data collection for network traffic began the moment the testbed was switched to operational mode. The attacks were performed at level 1 of the SWaT network as discussed in Section 2. The network data captures the communication between the SCADA system and the PLCs. Hence, the attacks were launched by hijacking the packets as they communicate between the SCADA system and the PLCs. During the process, the network packets are altered to reflect the spoofed values from the sensors.

Category	**Description**
Date	Date of Log
Time	Time of Log
Origin	IP of server
Type	Type of log
Interface Name	Network interface type
Interface Direction	Direction of data
Source IP	IP Address of source
Destination IP	IP address of destination
Protocol	Network Protocol
Proxy Source IP	Proxy address of Source
Application Name	Name of application
Modbus Function Code	Function Code
Modbus Function Description	Description of Modbus Function
Modbus Transaction ID	Transaction ID
SCADA Tag	Sensor or Actuator ID
Modbus Value	Value transmitted
Service/Destination Port	Port number of Destination IP
Source Port	Port number of Source IP

Table 3: Network Traffic Data

4.3 Labelling data

As the attacks performed in this paper were through a controlled process, labelling of the data turned out be straight forward. During the operation mode of the testbed, any actions to the testbed were required to be logged. Hence, all attacks performed for the purpose of data collection were logged with the information in Table 4.

Information	Description
Start time	Time when attack starts
End time	Time when attack ends
Attack Points	Sensors or actuator which will be compromised
Start State	Current status of the point
Attack	Description of attack
Attack Value	Substituted value of sensor (based on the attack)
Attacker's Intent	The intended affect of the attack

Table 4: Attack Logs

Labelling of physical properties Each data item corresponding to a sensor or an actuator data was collected individually into a CSV file. Each CSV file contains server name, sensor name, value at that point in time, time stamp, questionable, annotated and substituted. As the attributes are from the server, questionable, annotated and substituted are redundant and hence removed. All the remaining data was then combined into a single CSV file. Using attack logs, data was labelled manually based on the start and end-times of the attacks.

Labelling of Network Traffic The network data was separated into multiple CSV files with a line limit of 500,000 packets for easier processing. However, as the data was captured at per second interval, there are instances of overlap where multiple rows reflect a different activity but carry the same time stamp. Similarly, based on the attack logs, the data was labelled based on the end and start time of the attacks.

5 Conclusion

The lack of reliable and publicly available CPS datasets is a fundamental concern for researchers investigating the design of secure CPSs. There are currently no such large scale public datasets available as there are no open CPS facilities. Real industrial CPS facilities would not be able to provide accurate datasets as faults or attacks can only be assumed at best.

The data collected from the SWaT testbed reflects a real-world environment that helps to ensure the quality of the dataset in terms of both normal and attack data. The attacks carried out by the authors illustrate how such attacks can take place in modern CPSs and provide us the ability to provide accurately label data for subsequent use. The information and data that is provided with this paper includes both network and physical properties stored in CSV file formats.

Our goal is to make the collection of CPSs datasets an on-going process to benefit researchers. The data collected will be continuously updated to include datasets from new testbeds as well as new attacks derived from our research team.

Acknowledgments

This work was supported by research grant 9013102373 from the Ministry of Defense and NRF2014-NCR-NCR001-040 from the National Research Foundation, Singapore. The authors would like to thank Check Point® Software Technologies Ltd for the loan of their network equipment for data collection purposes.

References

1. Adepu, S., Mathur, A.: An investigation into the response of a water treatment system to cyber attacks. In: In Proceedings of the 17th IEEE High Assurance Systems Engineering Symposium (in Press) (2016)
2. Bay, S.D., Kibler, D., Pazzani, M.J., Smyth, P.: The uci kdd archive of large data sets for data mining research and experimentation. ACM SIGKDD Explorations Newsletter 2(2), 81–85 (2000)
3. Lippmann, R.: The 1999 darpa off-line intrusion detection evaluation. In: Computer Networks 34(4) 579-595, 2000. Data is available at http://www.ll.mit.edu/IST/ideval/ (2000)
4. Morris, T.: Industrial control system (ics) cyber attack datasets - tommy morris. `https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-set`, accessed: 2016-05-06